

NSM 2.2 Closed Network Feature Guide

SONICWALL®

Contents

Overview	2
About Network Security Manager	2
Closed Network Description	3
Conventions	4
Guide Conventions	4
UI Conventions	4
Related Documents	5
System Requirements	6
Browser Levels	6
Minimum System Configuration	6
MySonicWall	7
Firewall Types and Firmware	7
Deploying NSM	8
NSM Licensing	9
MSW Configuration	9
Enabling Closed Network	10
Associating the Nodes	11
Generating the Encrypted Files	11
Getting Started with the Closed Network NSM	13
Configuring Closed Network NSM	13
Adding Firewalls	14
SonicWall Support	15
About This Document	16

Overview

Welcome to the SonicWall NSM closed network Getting Started Guide. On-premises NSM (Network Security Manager) is an application that can configure and manage multiple SonicWall appliances from a central location. Using NSM in a closed network configuration, allows you the same unified management without being connected to the internet.

This guide contains installation procedures and configuration guidelines for a closed network deployment.

- [Overview](#)
- [System Requirements](#)
- [Deploying NSM](#)
- [NSM Licensing](#)
- [Getting Started with the Closed Network NSM](#)

About Network Security Manager

SonicWall Network Security Manager (NSM) is the next generation firewall management application that provides a holistic approach to security management. The approach is grounded in the principles of simplifying and automating various tasks to achieve better security operation and decision-making, while reducing the complexity and time required. NSM gives you everything you need for firewall management; it provides comprehensive visibility, granular control and the capacity to govern the entire SonicWall network security operations with greater clarity, precision and speed. This is all managed from a single, function-packed interface that can be accessed from any location using a browser-enable device. Firewalls can be centrally managed to provision all the network security services with a single-pane-of-glass experience.

This security management platform is a SaaS (Software-as-a-Service) or an on-premises offering, depending on your needs. The SaaS offering is accessible on-demand, via the cloud, with virtually unlimited system scalability to support multiple tenants with thousands of security nodes under each one. The solution's redundant and distributed architecture enables organizations to centrally and reliably manage a single small network to one or more enterprise-class deployments with the flexibility to scale without increasing management and administrative overhead.

The on-premises offering is for those customers that don't want to opt for a cloud solution. It can be deployed on multiple form factors such as ESXi and Hyper-V. The architecture allows you to scale to 10,000 devices under

management and supports a closed network implementation for those who need a network disconnected from the internet. Migration from Global Management System (GMS) is available in a future release.

Closed Network Description

Network administrators can use NSM in a management console role in an enterprise network containing SonicWall NSA, TZ, or SuperMassive appliances, and Email Security (ES) appliances.

On-premises NSM has been updated to work in a closed environment or closed network . In this scenario, NSM works with no direct access to back-end services. Typically, NSM automatically pulls all necessary files such as license key sets and signature files from the back-end server and pushes them to the firewalls. In a closed network case, NSM cannot reach the back-end servers so cannot access the key sets and signature files.

To maintain the closed environment, back-end files need to be manually delivered to the NSM system. MySonicWall first encrypts a package with all the necessary files. Then the encrypted package needs to be transferred to the NSM local file system so NSM can access the file.

① | **NOTE:** Unencrypted files are encrypted before making it a part of the compressed file.

Conventions

The *Network Security Manager Administration Guide* guide makes use of the following conventions:

- [Guide Conventions](#)
- [UI Conventions](#)



Guide Conventions










The following text conventions are used in this guide:

Convention	Use
Bold text	Used in procedures to identify elements in the user interface like dialog boxes, windows, screen names, messages, and buttons. Also used for file names and text or values you are being instructed to select or type into the interface.
Menu view or mode Menu item > Menu item	Indicates a multiple step menu choice on the user interface. For example, [[[Undefined variable Menu_Commands.Manager View]]] HOME > Firewall > Groups means verify you are in [[[Undefined variable Menu_Commands.Manager View]]] first and that the HOME option is selected. Then click on Firewall in the left-hand menu, and select Groups .
Computer code	Indicates sample code or text to be typed at a command line.
<i><Computer code italic></i>	Represents a variable name when used in command line instructions within the angle brackets. The variable name and angle brackets need to be replaced with an actual value. For example, in the segment <i>serialnumber=<your serial number></i> , replace the variable and brackets with the serial number from your device: <i>serialnumber=C0AEA0000011</i> .
Italic	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence, such as the first instance of a significant term or concept.

UI Conventions

When acquiring devices for management and reporting, the Status option uses colored icons to indicate the various states of the devices being monitored and managed.

Status Icon	Definition
	Indicates that a process is in progress. In some instances, specific details are provided: for example, Requesting Licenses.
	Indicates that a process has completed successfully. May provide a message indicating success or something with more detail.

Status Icon	Definition
	Indicates that a task is in process or pending the completion of another task. The message Pending is usually displayed, as well.
	Indicates a potential issue. Messages provide additional detail to help you resolve the issue.
	Indicates an error. Additional information may be provided via an information icon. Click the icon or mouse over it to see the message.
	Indicates an alert.
	Indicates the device is online.
	Indicates the device is offline.
	Indicates the device is unmanaged.
	Indicates the device is managed.
	Indicates that Zero Touch Connection is disabled for a device

Related Documents

The NSM documentation includes the following:

- *About Network Security Manager* provides an overview of the product and describes the base modes of operation, the navigation and icons, and the **Notification Center**.
- The *Network Security Manager Getting Started Guide* describes how to license and configure a basic NSM setup.
- The *NSM Administration Guide* reviews the management tasks for administering your security infrastructure.
- The *Network Security Manager Reporting and Analytics Administration Guide* discusses how to use the reporting and analytics features.
- *Network Security Manager On-Premises System Administration* describes the system administration tasks for an on-premises deployment of NSM.
- The *NSM Release Notes* summarizes the new features for the product.

System Requirements

The requirements for a Closed Network are the same as for any on-premises deployment. The minimum requirements are described in the following sections:

- [Browser Levels](#)
- [Minimum System Configuration](#)
- [MySonicWall](#)
- [Firewall Types and Firmware](#)

Browser Levels

Network Security Manager supports the following browsers:

Browser Supported	Notes
Google Chrome	Latest version ⓘ NOTE: This is the preferred browser for the real-time graphics display on the Dashboard.
Apple Safari	Latest version
Microsoft Edge	Latest version
Mozilla Firefox	Latest version

Minimum System Configuration

The minimum system configuration for a Closed Network system is:

Platform	Version	Configuration
----------	---------	---------------

VMware	ESXi 6.5	RAM: 24 GB
	ESXi 6.7	Core: 4 cores
	ESXi 7.0	
Hyper-V	Windows 2016	RAM: 24 GB
		Core: 4 cores
KVM	Linux Kernel 2.6.17 or above.	RAM: 24 GB
	Before installing KVM on Ubuntu, you have to verify if the hardware supports KVM. Availability of CPU virtualization extensions such as AMD-V and Intel-VT is the minimum requirement for installing KVM.	Core: 4 cores

MySonicWall

To log into Network Security Manager, you must have an active MySonicWall account. Go to mysonicwall.com to set up an account if you don't already have one.

Firewall Types and Firmware

The following firewall models can be managed by Network Security Manager .

	Gen 6	Gen 7
Entry Level Firewalls	SOHO W	TZ Series
	TZ Series	
	NSv 10-100	
Mid Range Firewalls	NSa 2600-6600	NSa 2700-6700
	NSa 2650-6650	NSv 270, 470
	NSv 200-400	
High-End Firewalls	SuperMassive 9000	NSv 870
	12K Series	NSsp 10700-15700
	NSa 9250-9650	
	NSv 800-1600	

Additional requirements include:

- The firewalls in the configuration must be a part of a tenant.

Deploying NSM

Setting up a Closed Network system follows the same process as for regular on-premises systems. Refer to the Getting Started Guides for the appropriate platform for details. The following provides a checklist for your implementation:

1. Download a copy of your image file from [MySonicWall](#).
2. Prepare your system for NMS installation. Steps may vary so refer to the appropriate Getting Started Guide for details.
3. Install and deploy NSM on your system.
4. Configure and enable Closed Network on MySonicWall. Refer to [NSM Licensing](#) for the details.
5. Configure your Closed Network on the NSM side. Refer to [Getting Started with the Closed Network NSM](#) for the details.

NSM Licensing

Topics: Licensing is important for the management of an NSM Closed Network. Since your NSM system won't have direct access to MySonicWall (MSW) through the internet, you need to define the devices that are associated with your NSM Closed Network license. When that done MSW builds a license package that you can transfer and install on your closed network.

Topics:

- [MSW Configuration](#)
- [Enabling Closed Network](#)
- [Associating the Nodes](#)
- [Generating the Encrypted Files](#)

MSW Configuration

The first step to setting up your Closed Network is to set up your licensing on MySonicWall.

1. Log in to [MySonicWall](#).
2. If your firewalls and NSM aren't already registered, navigate to **My Workspace > Register Products**.
3. Follow the steps in the wizard to register each of your products, including the firewalls in your NSM Closed Network setup.
4. Navigate to **Product Management > My Products** to confirm that they appear in your list.

Enabling Closed Network

Once all your devices and NSM is licensed on MSW, you need to enable the Closed Network feature.

1. Navigate to **Product Management > My Products** on MySonicWall.

#	RELEASE ST...	FRIENDLY NAME	SERIAL NUMBER	PRODUCT TYPE	REGISTERED ON ...	TENANT NAME	SUPPORT
1	ENABLED	0040100035B9_NSM	0040100035B9	NSM On-Prem	Mar 04 2021	SonicWall Technology	Mar 04 2022
2	ENABLED	0040100035AD_Secondary	0040100035AD	NSM On-Prem	Feb 23 2021	SonicWall Technology	Feb 23 2022
3	ENABLED	TEST_DEV_CLOSED_NETWORK_HA_P	0040100035AE	NSM On-Prem	Feb 23 2021	SonicWall Technology	Feb 23 2022

2. Click the icon to enable Closed Network (to the right).

Offline - Active Support

Serial Number 0040100035B9 Friendly name 0040100035B9_NSM

Tenant Name SonicWall Technology Systems India Private Ltd Products Registered On 04 Mar 2021

Node Support 5 Enable Closed Network

Support Expiration 04 Mar 2022 Description NSM MANAGEMENT ON-PREM BASE LICENSE - 5 NODES 1YR

Registration Code R4AWBS9B Authentication Code RCAF-KQSW

Registration Token + Firmware Version 2.2.0

Trusted YES Maintenance Key

GUID: [REDACTED] [Edit] [Delete]

TO-DO List
You have no pending tasks

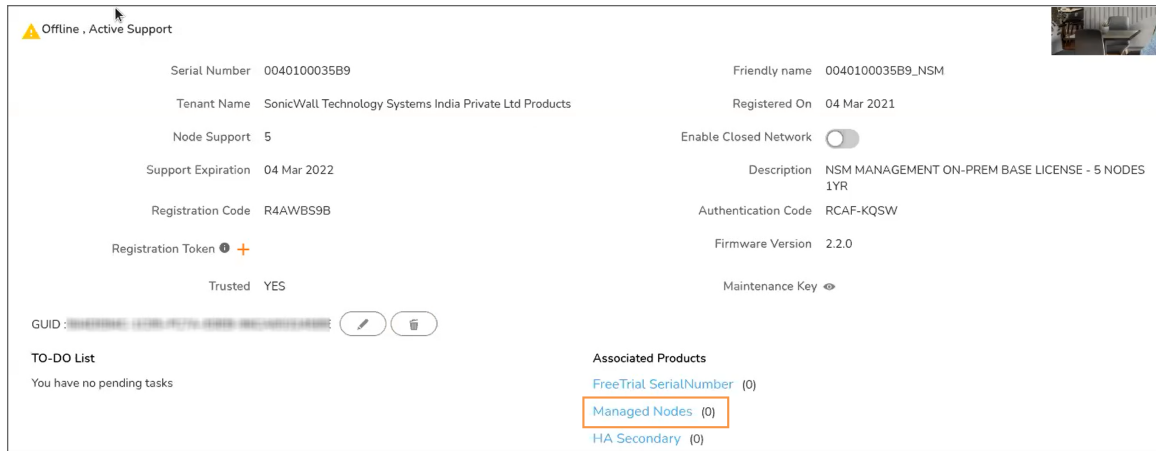
Associated Products
[FreeTrial SerialNumber \(0\)](#)
[Managed Nodes \(0\)](#)
[HA Secondary \(0\)](#)

3. Go to your NSM system and find the **GUID** on the dashboard. Note it for use in a later step.
4. Return to the MSW page and click the **Edit** icon next to the **GUID** field.
5. Enter the GUID in the popup and save it.
6. Click on Enable Closed Network. The switch turns into a link which is used later when generating your license files.

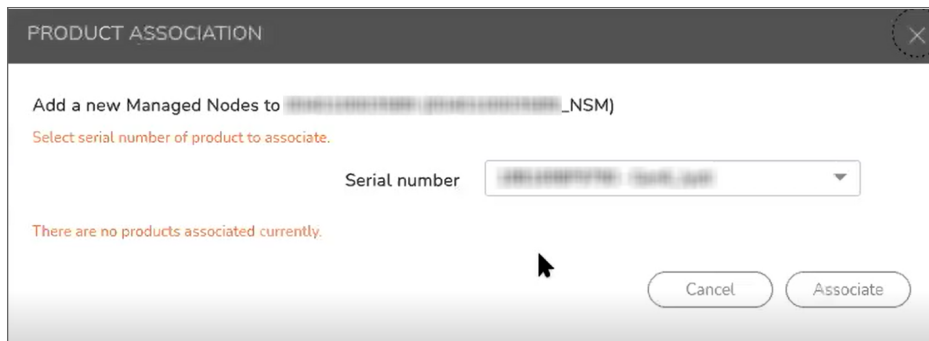
Associating the Nodes

After you enable Closed Network on NSM, you need to associate which firewalls are managed by NSM.

1. While still logged into MSW, navigate to the **Closed Network** page from **My Products**.



2. Click on **Managed Nodes**.

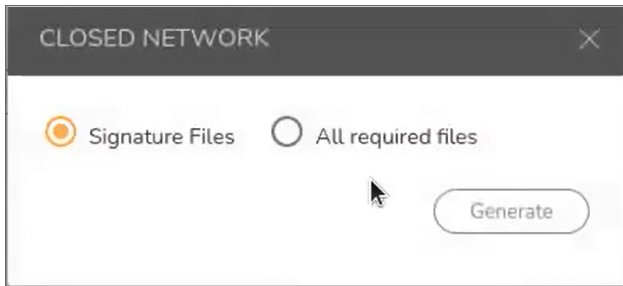


3. Select the serial number of the firewall to associate with the NSM.
4. Repeat if you additional firewalls to associate.

Generating the Encrypted Files

The final step to licensing the Closed Network NSM is to generate the encrypted files that you need to copy over to your NSM system.

1. While still logged into MSW, navigate to the **Closed Network** page from **My Products**, if not already there.
2. Click on the **Closed Network** link.



3. Select **All required files** and click **Generate**.
4. Accept the option to download the files and store where you can access them later from your NSM system.

Getting Started with the Closed Network NSM

After you complete the Closed Network setup on MySonicWall, you can go your NSM system to finish setting up your system. This section reviews how to get started with some basic configuration. Refer to the *Network Security Manager On-Premises System Administration* for more details about Closed Network and *NSM Administration Guide* for basic NSM configuration.

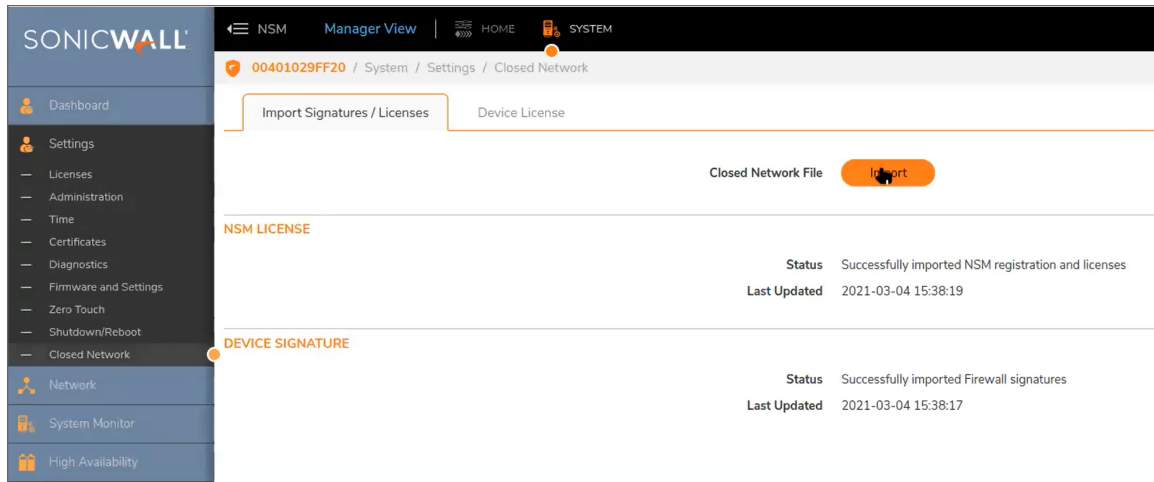
Topics:

- [Configuring Closed Network NSM](#)
- [Adding Firewalls](#)

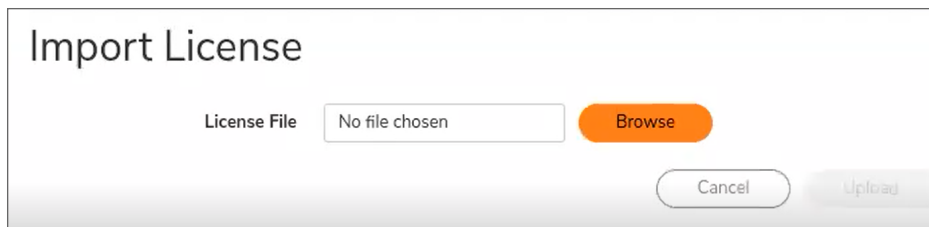
Configuring Closed Network NSM

After you complete the Closed Network setup on MySonicWall, you can go your NSM system to import the licenses.

1. Log in to your NSM system using your administrator credentials.
2. Navigate to **Manager View | HOME > Settings > Closed Network**.



3. On the **Import Signatures / Licenses** tab, click **Import**.



4. Click **Browse** to find your file on your system.
5. After selecting it, click **Upload**, and the system tells you when the file is successfully uploaded.
6. Navigate to **Manager View | HOME > Settings > Licenses** to confirm that Closed Network licenses were updated.
7. Refer to **Manager View | HOME > Settings > Closed Network** and select the **Device License** tab to see the devices managed by this NSM system.
 - ① | **NOTE:** The devices listed in the **Device License** tab are the same that are listed in MSW for this instance of NSM.

Adding Firewalls

After the licensing tasks have been completed on both the MSW and NSM sides, you add and manage the firewalls in the same way that you can in other configurations. The *NSM Administration Guide* provides the details for these task.

To start, you can go to **Manager View | HOME > Firewalls > Inventory** to add the firewalls and synchronize the devices. They will automatically register and the licenses will be pushed to the firewall.

- ① | **NOTE:** Zero Touch method of adding firewall is not supported for Closed Network deployment.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to <https://www.sonicwall.com/support>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at <https://community.sonicwall.com/technology-and-support>.
- View video tutorials
- Access <https://mysonicwall.com>
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit <https://www.sonicwall.com/support/contact-support>.

About This Document

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **TIP:** A TIP icon indicates helpful information.

⚠ | **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

⚠ | **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

Closed Network Feature Guide
Updated - January 2022
Software Version - 2.2
232-005624-00 Rev B

Copyright © 2022 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/legal/end-user-product-agreements/>.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035